Department of Defense

INSTRUCTION NUMBER 5200.40

December 30, 1997

ASD(C3I)

SUBJECT: DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

References:

(a) DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AISs),” March 21, 1988

(b) Public Law 100-235, “Computer Security Act of 1987,” January 8, 1988

(c) Office of Management and Budget Circular No. A-130, “Management of Federal Information Resources,” February 8, 1996

(d) Director of Central Intelligence 1/16, “Security Policy on Intelligence Information in Automated Systems and Networks,” March 14, 1988

(e) through (m), see enclosure E1.

1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures under reference (a) for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in the Department of Defense.

1.2. Creates the DoD IT Security Certification and Accreditation Process (DITSCAP) for security C&A of unclassified and classified IT to implement references (a) through (d).

1.3. Stresses the importance of a life-cycle management approach to the C&A and re-accreditation of DoD IT.

2. APPLICABILITY AND SCOPE

This Instruction:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the

Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"), their contractors, and agents.

2.2. Shall be used by milestone decision authorities when acquiring IT.

2.3. Shall apply to the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. It applies to any IT or information system life cycle, including the development of new IT systems, the incorporation of IT systems into an infrastructure, the incorporation of IT systems outside the infrastructure, the development of prototype IT systems, the reconfiguration or upgrade of existing systems, and legacy systems.

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure E2.

4. POLICY

This Instruction implements the policies defined in DoD Directive 5200.28, Pub. L. 100-235 (1987), OMB Circular A-130, DCID 1/16, and DoD Directive 5220.22 (references (a) through (e)).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Oversee and review implementation of this Instruction.

5.1.2. Review, oversee, and formulate overall policies that govern DoD security practices and programs to implement the DITSCAP as the standard DoD process for conducting IT C&A.

5.1.3. Promulgate standards, establish support and training, and manage the transition to the DITSCAP.

5.1.4. Conduct an annual assessment and/or review of the DITSCAP and consider proposed changes.

5.1.5. Ensure that each designated approving authority (DAA) implements and maintains the DITSCAP for security C&A of DoD Component and DoD contractor IT and networks under their jurisdiction.

5.2. The OSD Principal Staff Assistants and the Chairman of the Joint Chiefs of Staff, in respective areas of responsibility, shall ensure DoD Component compliance with the DITSCAP.

5.3. The Director, Defense Information Systems Agency shall:

5.3.1. Maintain DITSCAP procedural information in support of security C&A of DoD Component and DoD contractor IT systems and networks.

5.3.2. In coordination with the National Security Agency (NSA), implement, operate, and maintain an on-line information assurance support environment (IASE).

5.3.3. In coordination with NSA, provide assistance such as information system security engineering, security solutions, and security guidance to the DoD Components in the use of DITSCAP.

5.3.4. Provide DITSCAP training for the DoD Components.

5.3.5. Support the annual review of the DITSCAP.

5.4. The Heads of the DoD Components shall:

5.4.1. Implement the DITSCAP for security C&A of DoD Component and DoD contractor IT systems and networks in accordance with DoD Directive 5200.28, Pub. L. 100-235 (1987), OMB Circular A-130, DCID 1/16, DoD Directive 5220.22, DoD 5220.22-M, DoD 5220.22-M-Sup. and Chairman of the Joint Chiefs of Staff S3231.01 (references (a) through (h)) as applicable.

5.4.2. Provide assistance, and support to their respective Service or Agency constituents, in the implementation of the DITSCAP.

5.4.3. Assign responsibility to implement the standard C&A process to DAA responsible for accrediting each IT and network under their jurisdiction.

5.4.4. Support the annual review of the DITSCAP.

6. PROCEDURES

6.1. Approach. This Instruction defines the activities leading to security C&A. The activities are grouped together in a logical sequence. This Instruction presents the objectives, activities, and management of the DITSCAP process.

6.2. Objective. The objective of the DITSCAP is to establish a DoD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure (DII). The set of activities presented in the DITSCAP standardize the C&A process for single IT entities that leads to more secure system operations and a more secure DII. The process considers the system mission, environment, and architecture while assessing the impact of operation of that system on the DII.

6.3. C&A Process. The DITSCAP, enclosures E2. through E8., defines a process that standardizes all activities leading to a successful accreditation. The principal purpose of that process is to protect and secure the entities comprising the DII. Standardizing the process will

minimize risks associated with nonstandard security implementations across shared infrastructure and end systems. The IASE has been developed as the mechanism to support the implementation of the DITSCAP activities. The DITSCAP process shall consist of the following four phases:

6.3.1. Phase 1, Definition. The Definition phase shall include activities to document the system mission, environment, and architecture; identify the threat; define the levels of effort; identify the certification authority (CA) and the DAA; and document the necessary security requirements for C&A. Phase 1 shall culminate with a documented agreement, between the program manager, the DAA, the CA, and the user representative of the approach and the results of the phase 1 activities.

6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure E3., that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

6.3.4. Phase 4, Post Accreditation. The Post Accreditation phase shall include activities to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change management, and periodic compliance validation reviews are conducted.

6.4. Life-Cycle and Tailoring. The DITSCAP process applies to all systems requiring C&A throughout their life-cycle. It is designed to be adaptable to any type of IT system and any computing environment and mission. It may be adapted to include existing system certifications, evaluated products, use new security technology or programs, and adjust to the applicable standards. The DITSCAP may be mapped to any system life-cycle process but is independent of the life-cycle strategy. The DITSCAP is designed to adjust to the development, modification, and operational life-cycle phases. Each new C&A effort begins with phase 1, Definition, and ends with phase 4, Post Accreditation, in which follow-up actions ensure that the approved information system or system component continues to operate in its computing environment in accordance with its accreditation. The activities defined in these four phases are mandatory. However, implementation details of these activities may be tailored, and where applicable, integrated with other acquisition activities and documentation. Systems are categorizing into a set of system classes to support definition of standard security requirements and procedures, and to facilitate reuse of previous certification evidence.

7. INFORMATION REQUIREMENTS

7.1. The Systems Security Authorization Agreement (SSAA) Outline identified at enclosure E6., of this Instruction, is exempt from licensing in accordance with paragraph E.4.b, of DoD 8910.1-

M (reference (j)). The annual assessment to review and consider proposed changes to the standard C&A process, procedures and tools is exempt from licensing in accordance with paragraph E.4.c. of DoD 8910.1-M (reference (j)).

8. EFFECTIVE DATE

8.1. This Instruction is effective immediately.

8.2. This instruction shall be reviewed annually.

Enclosures - 8

1. References
2. Definitions
3. DITSCAP Description
4. Management Approach
5. Acronyms and Abbreviations
6. SSAA Outline
7. ITSEC System Class Description
8. DITSCAP Components Overview

E1. ENCLOSURE 1
REFERENCES, continued

(e) DoD Directive 5220.22, “Industrial Security Program,” November 1, 1986

(f) DoD 5220.22-M, “National Industrial Security Program Operating Manual,” January 1995, authorized by DoD Directive 5220.22

(g) DoD 5220.22-M-Sup, “National Industrial Security Program Operating Manual (NISPOMSUP),” December 29, 1994, authorized by DoD Directive 5220.22, December 8, 1980

(h) Chairman, Joint Chiefs of Staff S3231.01, “Safeguarding the Single Integrated Operational Plan (U),” November 30, 1993

(i) DoD Directive 5000.1, “Defense Acquisition,” March 15, 1996

(j) DoD 8910.1-M, “DoD Procedures for Management of Information Requirements,” November 28, 1986, authorized by DoD Directive 8910.1, June 11, 1993

(k) National Information Systems Security (INFOSEC) Glossary, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, August 1997 1

(l) Subsection 552a of title 5, United States Code

(m) Department of Defense Technical Architecture Framework for Information Management (TAFIM), Volume 6, DoD Goal Security Architecture (DGSA), 30 April 1996

1 Available from the National Security Telecommunications And Information Systems Security Committee Secretariat (V503), 9800 Savage Road STE 6716, Fort Meade MD 20755-6716.

2 Available from the DISA Information Systems Security Program Management Office, 701 Courthouse Road, Arlington, VA 22204-2199.

E2. ENCLOSURE 2
DEFINITIONS

E2.1. Terms

Terms used in this Instruction are selected from the NSTISSI 4009 (reference(k)) definitions when possible. Where new terms are used, the revised or new definitions will be submitted as changes to reference (k).

E2.1.1. Accountability. Property that allows auditing of IT system activities to be traced to persons or processes that may then be held responsible for their actions. Accountability includes authenticity and non-repudiation.

E2.1.2. Accreditation. Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

E2.1.3. Architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

E2.1.4. Acquisition Organization. The Government organization that is responsible for developing a system.

E2.1.5. Assurance. Measure of confidence that the security features, practices, procedures and architecture of an IT system accurately mediates and enforces the security policy.

E2.1.6. Authenticity. The property that allows the ability to validate the claimed identity of a system entity.

E2.1.7. Availability. Timely, reliable access to data and information services for authorized users.

E2.1.8. Certification. Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

E2.1.9. Certification Authority (CA). The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.

E2.1.10. Computing Environment. The total environment in that an automated information system, network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems.

E2.1.11. Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

E2.1.12. Confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices.

E2.1.13. Configuration Control. Process of controlling modifications to a IT system's hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

E2.1.14. Configuration Management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life-cycle of the IT.

E2.1.15. Configuration Manager. The individual or organization responsible for Configuration Control or Configuration Management.

E2.1.16. Data Integrity. The attribute of data that is related to the preservation of its meaning and completeness, the consistency of its representation(s), and its correspondence to what it represents.

E2.1.17. Defense Information Infrastructure (DII).
The DII is the seamless web of communications networks, computers, software, databases, applications, data, security services, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian

support, and wartime roles.

E2.1.18. Designated Approving Authority (DAA or Accreditor). Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk.

E2.1.19. Developer. The organization that develops the information system.

E2.1.20. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.

E2.1.21. Emissions security (EMSEC). Measures taken to deny unauthorized persons information derived from intercept and analysis of compromising emanations from crypto-equipment or an IT system.

E2.1.22. Environment. Aggregate of external procedures, conditions, and objects effecting the development, operation, and maintenance of an IT system.

E2.1.23. Evolutionary Program Strategies. Generally characterized by design, development, and deployment of a preliminary capability that includes provisions for the evolutionary addition of future functionality and changes, as requirements are further defined, DoD Directive 5000.1 (reference (i)).

E2.1.24. Governing Security Requisites. Those security requirements that must be addressed in all systems. These requirements are set by policy, directive, or common practice set; e.g., by E.O, OMB, the OSD, a Military Service or a DoD Agency. Those requirements are typically high-level. While implementation will vary from case to case, those requisites are fundamental and shall be addressed.

E2.1.25. Grand Design Program Strategies. Characterized by acquisition, development, and deployment of the total functional capability in a single increment, reference (i).

E2.1.26. Incremental Program Strategies. Characterized by acquisition, development, and deployment of functionality through a number of clearly defined system "increments" that stand on their own, reference (i).

E2.1.27. Information Category. The term used to bound information and tie it to an information security policy.

E2.1.28. Infrastructure-Centric. A security management approach that considers information systems and their computing environment as a single entity.

E2.1.29. Information Security Policy. The aggregate of public law, directives, regulations, rules, and regulate how an organization manages, protects, and distributes information. For example, the information security policy for financial data processed on DoD systems may be in U.S.C., E.O., DoD Directives, and local regulations. The information security policy lists all the security requirements applicable to specific information.

E2.1.30. Information System. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

E2.1.31. Information System Security Officer (ISSO). The person responsible to the DAA for ensuring the security of an IT system is approved, operated, and maintained throughout its life-cycle in accordance with the SSAA.

E2.1.32. Information Technology (IT). The hardware, firmware, and software used as part of the information system to perform DoD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

E2.1.33. Information Technology Security (ITSEC). Protection of information technology against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. Protection and maintenance of confidentiality, integrity, availability, and accountability.

E2.1.34. Integrator. An organization or individual that unites, combines, or otherwise incorporates information system components with another system(s).

E2.1.35. Integrity. Quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. It is composed of data integrity and system integrity.

E2.1.36. Legacy Information System. An operational information system that existed before to the implementation of the DITSCAP.

E2.1.37. Maintainer. The organization or individual that maintains the information system.

E2.1.38. Maintenance Organization. The organization that keeps an IT system operating in accordance with prescribed laws, policy, procedures and regulations. In the case of a contractor maintained system, the maintenance organization is the government organization responsible for, or sponsoring the operation of the IT system.

E2.1.39. Mission. The assigned duties to be performed by a resource.

E2.1.40. Non-Developmental Item (NDI). Any item that is available in the commercial marketplace; any previously developed item that is in use by a Department or Agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; any item described above, that requires only minor modifications

in order to meet the requirements of the procuring Agency; or any item that is currently being produced that does not meet the requirements of definitions above, solely because the item is not yet in use or is not yet available in the commercial market place.

E2.1.41. Other Program Strategies. Strategies intended to encompass variations and/or combinations of the grand design, incremental, evolutionary, or other program strategies, DoD Directive 5000.1 (reference (i)).

E2.1.42. Program Manager. The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system.

E2.1.43. Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

E2.1.44. Risk Assessment. Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.

E2.1.45. Risk Management. Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.

E2.1.46. Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

E2.1.47. Security Inspection. Examination of an IT system to determine compliance with security policy, procedures, and practices.

E2.1.48. Security Process. The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life-cycle.

E2.1.49. Security Requirements. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

E2.1.50. Security Specification. Detailed description of the safeguards required to protect an IT system.

E2.1.51. Security Test and Evaluation (ST&E). Examination and analysis of the safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system.

E2.1.52. Sensitive Information. Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (reference (l)), but that has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

E2.1.53. System. A set of interrelated components consisting of mission, environment, and architecture as a whole.

E2.1.54. System Entity. A system subject (user or process) or object.

E2.1.55. System Integrity. Quality of an IT system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

E2.1.56. System Security Authorization Agreement (SSAA). A formal agreement among the DAA(s), the CA, the IT system user representative, and the program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

E2.1.57. TEMPEST. Short name referring to investigation, study, and control of compromising emanations from IT

equipment.

E2.1.58. Threat. Any circumstance or event with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

E2.1.59. Threat Assessment. Formal description and evaluation of threat to an IT system.

E2.1.60. Trusted Computing Base (TCB). Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

E2.1.61. User. Person or process authorized to access an IT system.

E2.1.62. User Representative. The individual or organization that represents the user or user community in the definition of information system requirements.

E2.1.63. Utility. An element of the DII providing information services to DoD users. Those services include Defense Information Systems Agency Mega-Centers, information processing, and wide-area network communications services.

E2.1.64. Validation. Determination of the correct implementation in the completed IT system with the security requirements and approach agreed on by the users, acquisition authority, and the DAA.

E2.1.65. Verification. The process of determining compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and the DAA.

E2.1.66. Vulnerability. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.

E2.1.67. Vulnerability Assessment. Systematic examination of an information system or product to determine the

adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

E3. ENCLOSURE 3

DITSCAP DESCRIPTION

E3.1. DITSCAP OVERVIEW

E3.1.1. The DITSCAP establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit IT systems that will maintain the security posture of the DII. The DITSCAP focuses on protecting the DII by presenting an infrastructure-centric approach for C&A. The DITSCAP is designed to be adaptable to any type of IT and any computing environment and mission. The process should be adapted to include existing system certifications and evaluated products.

E3.1.2. The process is designed to certify that the IT system meets the accreditation requirements and that the system will continue to maintain the accredited security posture throughout the system life-cycle. The users of the process shall align the process with the program strategy and integrate the process activities into the system life-cycle. While DITSCAP maps to any system life-cycle process, its four phases are independent of the life-cycle strategy.

E3.1.3. The key to the DITSCAP is the agreement between the IT system program manager,3 the DAA, the CA, and the user representative. These managers resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the SSAA that is used to guide and document the results of the C&A. The objective is to use the SSAA to establish a binding agreement on the level of security required before the system development begins or changes to a system are made.

3 The term program manager will be used throughout this document to refer to the acquisition organization's program manager during the system acquisition, the system

manager during the operation of the system, or the maintenance organization's program manager when a system is undergoing a major change. The DAA is also referred to as the accreditor throughout this document.

Figure E3-1. The DITSCAP.

E3.2. DITSCAP PHASES

E3.2.1. The DITSCAP is composed of four phases: Definition, Verification, Validation, and Post Accreditation. (See figure E3-1.) Phase 1, Definition, is focused on understanding the mission, environment, and architecture to determine the security requirements and level of effort necessary to achieve accreditation. The objective of phase 1 is to agree on the intended system mission, environment, architecture, security requirements, certification schedule, level of effort, and resources required. Phase 2, Verification, verifies the evolving or modified system's compliance with the information agreed on in the SSAA. The objective of phase 2 is to produce a fully integrated system ready for certification testing. Phase 3, Validation, validates compliance of the fully integrated system with the information stated in the SSAA. The objective of phase 3 is to produce the required evidence to support the DAA in making an informed decision to grant approval to operate the system; e.g., accreditation. Phases 1, 2, and 3 are the DITSCAP process engine. Those phases are repeated as often as necessary to produce an accredited system. Phase 4, Post Accreditation, includes those activities necessary for the continuing operation of the accredited IT system in its computing environment and to address the changing threats a system faces through its life-cycle. Phase 4 starts after the system has been certified and accredited for operations. The objectives of phase 4 are to ensure secure system management, operation, and maintenance to preserve an acceptable level of residual risk.

E3.2.2. The phases are comprised of activities. The activities include various procedures and tasks. Each phase and activity shall be performed for every system. The procedures and tasks in each process activity may be tailored and scaled to the system and its associated acceptable level of residual risk. The procedures and tasks should be tailored and integrated with on-going

systems acquisition activities to best fit the mission, environment, system architecture, and programatic considerations. In that manner, the process maintains flexibility to deal with different acquisition strategies, and operational scenarios; e.g., rapid deployment.

E3.2.3. An ITSEC system class structure has been established, enclosure E7., that groups systems into classes to allow new developments to draw on previous experience. The system class approach makes it possible to establish class repositories to store information on other similar C&A efforts. As systems are certified and accredited, the approved solutions and documentation may be filed in a class repository. When a new system development begins, or an existing system is to be revised, the class repository may be accessed. That will facilitate rapid determination of system security policy and security requirements based on the group or class into that the system falls. The repository can also provide insight into the previous certification efforts and documentation of the approved solutions.

E3.2.4. The subparagraph E3.3. through E3.6., describe the process phases, activities, and tasks required. Enclosure E8. summarizes these process components. Additional details on the process may be found in the IASE. The IASE has been established to assist DITSCAP users in the use of the DITSCAP and to support the implementation of standard C&A practices throughout the Department of Defense.

E3.3. PHASE 1, DEFINITION

E3.3.1. Phase 1 tasks define the ITSEC C&A level of effort, identify the DAA and the CA, and culminate with an agreement, by the program manager, the DAA, the CA, and the user representative, on the method for implementing the security requirements. That agreement is documented in the SSAA, which shall describe the system mission, target environment, target architecture, security requirements, and applicable data access policies. The SSAA shall describe the applicable set of planning and certification actions, resources, and documentation required for the C&A. The SSAA is the vehicle that guides the implementation of ITSEC requirements and the resulting C&A actions. The SSAA outline, enclosure E6., lists information

that should be included.

E3.3.1.1. Phase 1, figure E3-2, contains three process activities, document mission need, registration, and negotiation. Phase 1 starts with the input of the mission need statement (or other justification for the system) and ends by producing the SSAA. The process activities provide the pathway to understanding the IT system requiring C&A; documenting the ITSEC requirements; developing a security architecture approach; and determining the scope, level of effort, documentation required, and schedule for the planning and certification actions. Any level of change to existing systems shall initiate the process. During the registration and negotiation activities, the program manager, the DAA, the CA, and the user representative will determine what actions shall follow that system change.

Figure E3-2. DITSCAP Phase 1 Definition Activities.

E3.3.2. Document Mission Need. Documenting mission need is the process activity that initializes the DITSCAP. Initialization occurs when an information system is developed or modified in response to an identified operational requirement or mission need. The mission need, figure E3-3, is either a document or compilation of information stating the requirements of the system and describing its intended capabilities. Those capabilities include functions the system should perform, desired interfaces and capabilities associated with those interfaces, the information to be processed, the operational organizations supported, the intended operational environment, and the operational threat. Typically, the mission need is described in a high-level requirements document before the DITSCAP is initiated.

Figure E3-3. Mission Need Security Relevant Information.

Mission Need Statement

1. System mission, functions, and system interfaces.

2. Operational Organization.

3. Information category and classification.

4. Expected system life-cycle.

5. System users characteristics.

6. Operational environment.

E3.3.3. Registration. Registration is the process activity in phase 1 that initiates the dialogue among the program manager, the DAA, the CA, and the user representative. As part of the Registration tasks, information is collected and evaluated, applicable ITSEC requirements are determined, risk management and vulnerability assessment actions begin, and the level of effort required for C&A is determined and planned. Registration shall begin with a review of the mission need and concludes with preparation of an initial draft of the SSAA.

Figure E3-4. Tasks Performed During Registration.

Registration Tasks

1. Inform the DAA, the CA, and the user representative that the system will require C&A support; e.g., register the system.

2. Prepare mission description and system identification.

3. Prepare the environment and threat description.

4. Prepare system architecture description and C&A boundary.

5. Determine ITSEC system class.

6. Determine the system security requirements.

7. Identify organizations that will be involved in the C&A and identify resources required.

8. Tailor the DITSCAP tasks, determine the C&A level-of-effort, and prepare a DITSCAP plan.

9. Develop the draft SSAA.

E3.3.3.1. Registration tasks, figure E3-4, guide the collection of necessary information to address the process

in a repeatable, understandable, and effective manner.
Those tasks identify information necessary for determining security requirements and the level of effort to accomplish the C&A that is influenced by the degree of assurance needed in the areas of confidentiality, integrity, availability, and accountability. Registration shall consider the system development approach, system life-cycle stage, existing documentation, mission, environment (including the threat assessment), architecture, users, data classification and categories, external interfaces, and mission criticality.
Mission-system relationships may vary from a single system supporting a single mission, to a single system supporting multiple missions, to a multiple systems supporting multiple missions, to a multiple systems supporting a single mission. A crucial piece of information for the accreditation is the identification of the roles that the system shall support in the encompassing enterprise mission.

E3.3.3.2. Most of that information can be obtained from examining the mission need and functional requirement documents. That information is used to determine the system class (see enclosure E7.). The various system classes are associated with minimum-security requirements and specific actions that shall be performed. The system class approach establishes minimum-security requirements as a function of mission(s), environment, and system architecture. The DITSCAP provides the capability to normalize high-level requirements through the use of the system class structure. The system class approach supports the identification of other similar systems that have undergone C&A, to analyze previously approved security requirements and solutions. That supports the reuse of their security requirement definitions, draws from their architecture approaches, and promotes reuse of applicable C&A information. Determining the applicable system class is essential to the development of the minimal security requirements necessary for the certification and eventual accreditation of the system.

E3.3.3.3. A key task in registration is to prepare an accurate description of the system and its development, operating and maintenance environment under consideration.
While the details of the system or the environment may not be clear at the onset of a system development, the system shall be defined in enough detail to accurately

portray the system's general concept and boundaries. That description shall define what is included in the accreditation boundary (e.g. system boundary, facilities, and equipment), and the external interfaces with other equipment or systems. Currently known threats shall be assessed against the specific system mission and a description to determine the necessary protection required. The threat, and subsequent vulnerability assessments, shall be used in establishing and selecting the ITSEC policy objectives that will counter the threat.

E3.3.3.4. The key roles in the DITSCAP are the program manager of the organization responsible for the system, the DAA, the CA, and the user representative. As a system progresses through the life-cycle phases, system responsibility (engineering and funding) may change. During acquisition, that responsibility may be the acquisition organization that will be represented by the system's program manager. During the operations and maintenance phase of the system, that responsibility may be the system manager or in the case of a major upgrade, the maintenance organization who will be represented by the upgrade program manager. The DAA is usually a senior operational commander with the authority and ability to evaluate the system operations in view of the security risks. The CA, security teams, etc. are the technical experts that support the C&A process. The system users may be part of a single organization or a large diverse community. In either case, for DITSCAP purposes, the user representative will represent their interests.

E3.3.3.5. To maintain the goal of a standard DoD process, the DITSCAP was developed in a manner that it can readily be applied to any system program strategy, (grand design, incremental, evolutionary, etc.) or life-cycle management process, DoD Directive 5000.1 (reference (i)). During phase 1, the application of the DITSCAP shall be tailored to the system program strategy, the life-cycle management process, and to adjust to systems that have progressed in their life-cycle. Tailoring adapts the security tasks to the system's life-cycle phase and program strategy. The process generally has been described as if it were to be applied to a new system with a grand design program strategy. In that case the DITSCAP phase 1 would be initiated during the phase 0, concept exploration

and definition phase, and tailored to support the ensuing system milestone decisions. Legacy systems shall enter the DITSCAP process when they are in need of compliance validation or undergo a modification that may impact the security posture. For example, if the system is in the operations and support phase, and the IT system is not accredited, the DITSCAP would be initiated with phase 1. The process would be tailored, the SAA would developed, and on agreement between the system program manager, the DAA, the CA, and the user representative, the process would move to applicable phase 2 and phase 3 activities. That capability permits the certification effort to be scaled to fit the size and complexity of the system while remaining responsive to the operational requirements driving the information system development or modification. The certification analysis tasks can be tailored to work with all DoD program strategies.

E3.3.3.6. Certification tasks, based on analysis of the characteristics of the IT and the security requirements, are defined for each system class. Certification tasks are grouped into four certification levels to provide guidance on the recommended minimum tasks. Use of enclosure E7. is strongly recommended as the method to determine the certification level. The DAA, the CA, the program manager, and the user representative may tailor the certification tasks and level of effort to the IT system mission, environment, architecture, programmatic considerations, and level of acceptable risk. For example, the three managers may choose to condense the time scale to meet operational needs, or to use previously approved security solutions and reduce the corresponding certification tasks. As the system development or maintenance progresses, new issues may emerge, and phase 1 may be revisited for new agreements or additional tailoring. The DAA, the CA, the program manager, and the user representative each represent different views and as such provide the checks and balances to ensure the minimum-security requirements are met. Therefore, it is important the SSAA be kept current to reflect each of these tailoring decisions.

E3.3.3.7. The SSAA is prepared during registration. The preparation of the SSAA shall have all parties involved or represented, including the CA, program sponsor, threat specialist, etc. When registration planning

activities are concluded, the draft is submitted to the DAA, the program manager, and the user representative. The draft SSAA is used as a guide to establish the basis for discussions during the negotiation activities among the DAA, the CA, the program manager, and the user representative.

E3.3.4. Negotiation. Negotiation is the process activity of the DITSCAP, where all the participants involved in the information system's development, acquisition, operation, security certification, and accreditation agree on the implementation strategy to be used to satisfy the security requirements identified during system registration. The key parties who must reach agreement during the negotiations are the program manager, the DAA, the CA, and the user representative. 4 The negotiation tasks are shown in figure E3-5.

Figure E3-5. Negotiation Tasks.

Negotiation Tasks

1. Review initial SSAA.

2. Conduct the certification requirements review.

3. Approve final SSAA.

E3.3.4.1. A review of the initial SSAA is performed by the DAA. The DAA shall conduct a complete review of the draft SSAA and all aspects that may impact C&A. The CA is responsible for the comprehensive evaluation of the technical and nontechnical security features of the IT. The CA is regarded as the technical expert in the discussions that consider tradeoffs between security requirements, cost, availability, and schedule to manage security risk.

4 It is recognized these managers may chose to designate someone to represent them in the negotiations. (In some cases the DAA may designate the CA to act in his or her behalf.) Unless noted otherwise, the terms will be used interchangeably to mean the principle or their designated representative.

E3.3.4.2. A certification requirements review (CRR)

shall be held for the principals involved in the C&A process. As a minimum, the program manager, the user representative, the DAA, and the CA shall attend the CRR. The review shall include the information documented in the SSAA; i.e., mission and system information, operational and security functionality, operational environment, system class, security policy, system security requirements, known security problems or deficiencies, and other security relevant information. While that review may be held with other system reviews, the intent of the CRR is to assist the organization responsible for IT system in preparing for the certification actions. The CRR review shall result in an agreement regarding the level of effort and the approach that will be taken to implement the security requirements.

E3.3.4.3. Negotiation is NOT a consideration of which security requirements to implement and which to delete. For example, any system connected to the DII, or any network, shall comply with the connection rules for those systems that it is to be connected. The purpose of negotiation is to ensure that all participants understand their roles and responsibilities and that the SSAA properly and clearly defines the approach and level of effort. Negotiation ends when the responsible organizations adopt the SSAA and concur that those objectives have been reached.

E3.3.5. SSAA. The objectives of the SSAA, shown in figure E3-6, are to document the conditions of C&A for an IT system. The SSAA is a formal agreement among the DAA(s), the CA, the IT system user representative, and the program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify ITSEC requirements, document certification tailoring and level of effort,5 identify possible solutions, and maintain operational systems security. The SSAA shall identify all costs relevant to the C&A process and the program manager shall add a C&A funding line item to the program budget to ensure the funds are available. Funding shall cover any travel or program contractor costs associated with certification, test development, testing and accreditation. Where multiple accreditors may be involved, an agreement between the accreditors may be necessary. That agreement must be included with the SSAA. Since the SSAA is an agreement among

Government entities, to be binding on the government's contractors, the provisions must be included in contractual documents between the Government and any contractors.

5 Supporting C&A teams may be useful to support the accreditor.

Figure E3-6. SSAA Objectives.

SSAA

1. Document the formal agreement among the DAA(s), the CA, the user representative, and the program manager.

2. Document all requirements necessary for accreditation.

3. Document all security criteria for use throughout the IT system life-cycle.

4. Minimize documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations (CONOPS), plans, architecture description, etc.).

5. Document the DITSCAP plan.

E3.3.5.1. The SSAA is intended to reduce the need for extensive documentation by consolidation of security related documentation into one document. That eliminates the redundancy and potential confusion as multiple documents describe the system, security policy, system and security architecture, etc. When feasible, the SSAA can be tailored to incorporate other documents as appendices or by reference to the pertinent document. An outline of the SSAA is found in enclosure E6.

E3.3.5.2. Each IT system shall have a SSAA. The physical characteristics of the SSAA will depend on the system class and level of effort needed for C&A. The SSAA can be as simple as a single coordinated message or as complex as a detailed system security plan. For generic accreditation’s, a single SSAA may be prepared for the system, but the description of the operating environment will need to reflect each proposed operation location. The goal is to produce a SSAA that will be the basis of agreement throughout the system's life-cycle.

E3.3.5.3. The four parties to the negotiation have the authority to tailor the SSAA to meet the characteristics of the IT, operational requirements, security policy, and prudent risk management. The SSAA must be flexible enough to permit adjustment throughout the system's life-cycle as conditions warrant. New requirements may emerge from design necessities, existing requirements may need to be modified, or the DAA's overall view of acceptable risk may change. When that occurs, the program manager, the DAA, the CA, and the user representative shall ensure the SSAA is updated to accommodate the new components. Common sense must be applied to the rules. The SSAA is developed in phase 1 and updated in each phase as the system development progresses and new information becomes available. In this sense, the SSAA is regarded as a living document. The completed SSAA contains those items that must be agreed on by the DAA, the CA, the user representative, and the program manager. The support organizations must understand each of these essential items.

E3.4. Phase 2, Verification.

The process activities of phase 2 verify the evolving system's compliance with the requirements agreed on in the SSAA. (See figure E3-7.) That phase consists of those process activities that occur between the signing of the initial version of the SSAA and the formal C&A of the system. Phase 2 process activities include continuing refinement of the SSAA, system development or modification, certification analysis, and analysis of the certification results.

E3.4.1. Refine the SSAA. Phase 2 starts with a review of the SSAA. All participants shall at minimum, read the SSAA. A detailed review shall be completed if there has been considerable time delay since the completion of phase 1, or if new people are now involved in the C&A. That review continues throughout phase 2 as the development or modification of the system progresses.

At each stage of the development or modification, the SSAA shall be refined by adding details to reflect the current state of the system. Any changes in the system that affect its security posture must be submitted to the DAA, the CA, the program manager, and the user

representative for approval and execution in the revised SSAA. As the development or modification progresses and specific information on to the certification effort becomes available, the SSAA shall be updated to include more specific details. At each subsequent stage of the IT system's development or modification, increasing details about the hardware and software architecture become available. That design information shall be added to the SSAA as justification to support the agreed on level of certification actions.

Figure E3-7. DITSCAP Phase 2, Verification Activities.

E3.4.2. System Development Activity. System development activities are those activities required to develop and integrate the IT system components. The specific activities are a function of the overall program strategy, the life-cycle management process, and the position of the information system in the life-cycle. The certification analysis activity in phase 2 is intended to ensure that the requirements of the SSAA are followed during each life-cycle phase of the development and modification of the information system. Each system development activity task has a corresponding phase 2 certification analysis task. The system development activity and certification analysis tasks ensure that the requirements in the SSAA are met.

E3.4.3. Certification Analysis. Certification analysis is the process activity that determines if the IT system is ready to be evaluated and tested under phase 3, validation. Because the DITSCAP is a success-oriented process, this process activity ensures that the development, modification, and integration efforts will result in a certifiable and accreditable information system before phase 3 begins.

E3.4.3.1. The certification analysis tasks that occur during the process activity, certification analysis, are shown in figure E3-8. Those certification tasks verify by analysis, investigation, and comparison methodologies that the IT design implements the SSAA requirements and that the IT components that are critical to security function properly. Those tasks compliment the functional testing certification tasks that occur during phase 3. While every system may be considered certifiable,

the goal is to produce systems with an acceptable level of risk.

Figure E3-8. Certification Tasks During Verification.

Certification Tasks

1. System architecture analysis.

2. Software design analysis.

3. Network connection rule compliance analysis.

4. Integrity analysis of integrated products.

5. Life-cycle management analysis.

6. Vulnerability assessment.

E3.4.3.2. As a result of completion of the phase 2 certification analysis, the system should have a documented security specification, a comprehensive test plan, and written assurance that all network and other interconnections requirements have been implemented. Commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products used in the system design shall have been validated to assure that they have been integrated properly and that their functionality meets the security needs of the system. A vulnerability assessment will have been conducted and will have concluded that the infrastructure needs of the system; e.g., configuration management, will be accommodated throughout the IT life-cycle. On acceptance of the vulnerability assessment, the C&A task proceeds to phase 3, that contains the formal system certification test and security accreditation actions.

E3.4.3.3. All analysis tasks, applicable for that system class, are to be completed. The intensity of the certification analysis tasks are scaled to the complexity of the IT design, the sensitivity of the information processed, and the criticality of the information system's intended mission. The specific certification tasks may be tailored to the IT program strategy, its life-cycle management process, and the position of the information system in its life-cycle. Certification tasks are tailored

to the system development activities to ensure that the former are relevant to the process and provide the required degree of analysis to ensure conformance with the SSAA. Tailoring also gives DITSCAP the flexibility to adjust the level of effort to fit the operational need. In that manner, tailoring permits the DITSCAP to remain responsive to national agency and military department priorities. Phase 2 certification tasks may vary from completion of a minimal checklist to in-depth analysis as determined by the system class.emsp; The certification tasks are discussed in paragraphs E3.4.3.3.1 through E3.4.3.3.6. below.

E3.4.3.3.1. System Architecture Analysis. The objective of this certification task is to ensure that the system architecture complies with the architecture description agreed on in the SSAA. Analysis of system level information reveals how effectively the security architecture implements the security policy and requirements. The interfaces between this and other systems shall be identified. Those interfaces must be evaluated to assess their effectiveness in maintaining the security posture of the infrastructure.

E3.4.3.3.2. Software Design Analysis. The software design certification task shall evaluate how well the software reflects the security requirements of the SSAA and the security architecture of the system. That certification task may include a detailed analysis of software specifications and software design documentation. The TCB shall be identified and analyzed for proper and full implementation of the security requirements. The task shall assess whether the critical security features e.g., identification and authentication, access controls, and auditing, are implemented correctly and completely.

E3.4.3.3.3. Network Connection Rule Compliance Analysis. The connection of an information system to a network requires that the particular system will not adversely affect the security posture of the network. Connection also requires that the network will not adversely affect the IT system's own security posture. That certification task evaluates the intended connections to other systems and networks to ensure the system design will enforce specific network security policies and protect the IT

system from adverse confidentiality, integrity, availability, and accountability impacts.

E3.4.3.3.3.1. Network analysis may include the evaluation of intended interfaces for compliance with the security connection rules not only for the network, but also for the information system. The system concept of operations (SSAA section 1) shall be examined to identify all the connections and interfaces intended for the system. It is important to determine if connections exist that were not in the initial concept, but are to be added after the initial fielding or modification of the system. The interfaces to the networks or to other systems shall be evaluated to determine if the system and network security can be maintained at both ends of the interface. They also shall be evaluated to ensure that end-to-end connection constructs are maintained and security connection rules are applied. Test plans and procedures shall be developed to validate compliance with the network connection rules.

E3.4.3.3.4. Integrity Analysis of Integrated Products (COTS, GOTS, or Non-Developmental Item (NDI. This certification task evaluates the integration of COTS, GOTS, or NDI software, hardware, and firmware to ensure that their integration into the system design complies with the system security architecture, and the integrity of each product is maintained.

E3.4.3.3.4.1. Integrated product analysis shall include the identification, and may include the verification of the security functionality, of each product. That certification task shall determine whether or not evaluated products are being used for their intended purpose. Integrity product analyses shall include an examination of the system and subsystem interfaces, information flows, and applicable use of selectable product features. All interfaces and information flows are examined to identify how they access the products.

E3.4.3.3.5. Life-Cycle Management Analysis. This certification task ensures that change control and configuration management practices are, or will be, in place and are sufficient to preserve the integrity of the security relevant software and hardware. During the system development, or maintenance, the development approach,

procedures, and engineering environment are assessed and the life-cycle plans are evaluated. Proposed contingency, continuity of operations, and back-up plans shall be evaluated for feasibility. That may require examining the following types of documents or procedures shown in figure E3-9.

Figure E3-9. Life-Cycle Management Documentation.

Life-Cycle Management Documentation

1. Computer Resource Management Plan (CRMP).

2. Computer Resources Life-Cycle Management Plan (CRLCMP).

3. Configuration identification procedures.

4. Configuration control procedures.

5. Configuration status accounting procedures.

6. Configuration audit procedures and reports.

7. Software engineering (development approach and engineering environment) procedures.

8. Trusted distribution plans.

9. Contingency, continuity of operations, and back-up plans.

E3.4.3.3.6. Vulnerability Assessment. This certification task shall evaluate security vulnerabilities with regard to confidentiality, integrity, availability, and accountability and recommends applicable countermeasures. The DAA should determine the acceptable level of risk to protect the system commensurate with its value to the Department of Defense. 6 In phase 2, the vulnerability assessment concentrates on the progress in implementing the security requirements of the SSAA. It reviews the SSAA at the beginning of phase 2 and concludes with notifying the CA and the DAA that the information system is ready for C&A evaluation and testing.

E3.4.3.3.6.1. During vulnerability assessment, each of the vulnerabilities and discrepancies isolated during

the evaluation of the system architecture, system design, network interfaces, product integration, and configuration management practices is analyzed to determine its susceptibility to exploitation, the potential rewards to the exploiter, the probability of occurrence, and any related threat. The analysis should use techniques such as static penetration, or active penetration testing to determine the ability to exploit the vulnerabilities. The residual risk, that portion of risk that remains after security measures have been applied, shall be determined by ranking the evaluated vulnerabilities against threat, ease of exploitation, potential rewards to the exploiter, and a composite of the three areas. All residual risks shall be identified and evaluated. The evaluation shall indicate the rationale as to why the risk should be accepted or rejected, and the operational impacts associated with these risks.

E3.4.3.3.6.2. Coordination among the program manager, the DAA, the CA, and the user representative ensures that the residual risk does not exceed the level of risk established by the DAA. That level of risk that shall now be documented in the SSAA is called the "acceptable level of residual risk." If the risk exceeds the maximum acceptable risk, the system shall fail the C&A.

6 An acceptable level of residual risk is based on the relationship of the threat to the system and the information processed, to the information system's mission, environment, and architecture; and its security confidentiality, integrity, availability, authenticity, and nonrepudiation objectives.

E3.4.4. Assess Analysis Results. At the conclusion of each life-cycle development milestone, the certification analysis results are reviewed for SSAA compliance. If the results indicate significant deviation from the SSAA, the DITSCAP shall revert to phase 1 to resolve the problems. If the results are acceptable, the DITSCAP proceeds to the next development task or to government acceptance and security testing; i.e., DITSCAP phase 3.

Figure E3-10. DITSCAP Phase 3, Validation Activities.

E3.5. Phase 3, Validation.

Phase 3 process activities, shown in figure E3-10, validate that the preceding work has produced an information system that operates in a specified computing environment with an acceptable level of residual risk. This phase consists of process activities that occur after the system is integrated and culminates in the accreditation of the IT system. Phase 3 includes a review of the SSAA, an evaluation of the integrated IT system, certification, and accreditation.

E3.5.1. Refine the SSAA. Phase 3 begins with a review of the SSAA to ensure that its requirements and agreements still apply. That review shall continue throughout phase 3 as the integrated system is subjected to successive levels of evaluation. At each stage of the integrated IT system's acceptance, the SSAA shall be refined by adding details to reflect the current state of the system. Required changes shall be submitted to the DAA, the CA, the program manager, and the user representative so that the revised agreement may be approved and executed.

E3.5.2. Certification Evaluation of the Integrated System. This process activity is to certify that the fully integrated and operational system complies with the requirements stated in the SSAA and may be operated with an acceptable level of residual risk. During this process activity, certification tasks, shown in figure E3-11 are performed on the integrated operational system to ensure that the IT system is functionally ready for operational deployment. The certification tasks and the extent of the tasks will depend on the level of certification analysis agreed on in the SSAA.

E3.5.2.1. Phase 3 certification tasks shall include certification of the software, firmware, and hardware and inspections of operational sites to ensure their compliance with the physical security, procedural security, TEMPEST, and COMSEC requirements. Phase 3 includes tasks to certify the compatibility of the computing environment with the description provided in the SSAA. DITSCAP flexibility permits the certification actions to be scaled to the type of IT system being evaluated and tailored to the program strategy used in the development or modification of the system. Subparagraphs E3.5.2.1.1. through E3.5.2.8. describe the certification tasks that

may be included in the evaluation of the integrated system.

Figure E3-11. Certification Tasks During Validation.

Certification Tasks

1. Security Test and Evaluation.

2. Penetration testing.

3. TEMPEST and Red-Black verification.

4. Validation of COMSEC compliance.

5. System management analysis.

6. Site accreditation survey.

7. Contingency plan evaluation.

8. Risk-based management review.

E3.5.2.1.1. System Security Test and Evaluation. The objective of the ST&E is to assess the technical and non-technical implementation of the security design and to ascertain that security features affecting confidentiality, integrity, availability, and accountability have been implemented in accordance with the SSAA, and perform properly. System ST&E shall validate the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance. Individual tests shall evaluate system conformance with the requirements, mission, environment, and architecture defined in the SSAA. Test plans and procedures shall address all the security requirements and the results of the testing will provide sufficient evidence of the amount of residual risk. These results shall validate the proper integration and operation of all security features.

E3.5.2.1.1.1. When a system is deployed to multiple locations, the ST&E may occur at a central integration and test facility. When use of such a facility is not possible, the integrated system may be tested at one of the intended-operating sites. Software and

hardware security tests of common system components at multiple sites are not recommended. The system installation and security configuration should be tested at operational sites.

E3.5.2.1.2. Penetration Testing. For applicable system classes, penetration testing is strongly recommended to assess the system's ability to withstand intentional attempts to circumvent system security features by exploiting technical security vulnerabilities. Penetration testing may include insider and outsider penetration attempts based on common vulnerabilities for the technology being used.

E3.5.2.1.3. TEMPEST and Red-Black Verification. TEMPEST and Red-Black verification may be required to validate that the equipment and site meet the security requirements. In these situations the site may be inspected to determine if adequate practices are being followed, and the equipment may be subjected to TEMPEST testing.

E3.5.2.1.4. Validation of COMSEC Compliance. This certification task validates that COMSEC approval has been granted and approved COMSEC key management procedures are used. COMSEC analysis evaluates how well the SSAA defined COMSEC requirements are integrated into the system architecture and the site management procedures.

E3.5.2.1.5. System Management Analysis. The system management infrastructure shall be examined to determine whether it adequately supports the maintenance of the environment, mission, and architecture described in the SSAA. Infrastructure components, that may provide insight into security of operations at the site, include the system and security management organizations, security training and awareness, and the configuration management organization and processes. The roles and responsibilities assigned to ISSO shall be examined to ensure that the responsibilities are consistent with the procedures identified in the SSAA. The system and security management organization shall be examined to determine the ability of the ISSO to report security incidents and implement security changes.

E3.5.2.1.5.1. Knowledge of the security management

structure may provide insight into the emphasis the organization places on secure operation of the computing environment. It also shall provide an indication of effectiveness of the security personnel. Security training and awareness shall be examined to provide insight into potential security problem areas.

E3.5.2.1.5.2. An effective configuration management program is mandatory if an established secure posture is to be maintained. This certification task evaluates the change control and configuration management practices to determine their ability to preserve the integrity of the security relevant software and hardware. A system baseline that identifies all information hardware, software, and firmware components and external interfaces, provides for future security evaluations and establishes a known reference point from which to make future accreditation decisions. Configuration management practices shall include periodic reverification of the system configuration to ensure unauthorized changes have not occurred.

E3.5.2.1.6. Site Accreditation Survey. The site accreditation survey task shall ensure that the site operation of the information system is accomplished in accordance with the SSAA. The site accreditation survey shall validate that the operational procedures for the IT, environmental concerns, and physical security pose no unacceptable risks to the information being processed. Where the IT system may not be confined to a fixed site; i.e., tactical or mobile systems and embedded system in ships or aircraft, the IT system shall be examined in representative sites or environments.

E3.5.2.1.7. Contingency Plan Evaluation. The contingency plan evaluation task analyzes the contingency, back-up, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA. Periodic testing of the contingency plan is required by DoD Directive 5200.28 (reference (a)) for critical systems and is encouraged for all systems.

E3.5.2.1.8. Risk Management Review. The risk-based management review task assesses the operation of the system to determine if the risk to confidentiality, integrity, availability, and accountability is being maintained at an acceptable level. The risk management

review shall assess the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. The operational procedures and safeguards shall be evaluated to determine their effectiveness and ability to offset risk. This is the final review before developing the recommendation to the DAA.

E3.5.3. Develop Recommendation to the DAA. This process activity begins after completion of all certification tasks and ends with the accreditation decision by the DAA. The purpose is to consolidate the findings developed during certification of the integrated system, submit the CA's report to the DAA, and produce the DAA accreditation decision.

E3.5.3.1. CA's Recommendation. If the CA concludes that the integrated IT satisfies the SSAA technical requirements, the CA issues a system certification. That is a certification that the IT system has complied with the agreed on security requirements. Supplemental recommendations also might be made to improve the system's security posture. Such recommendations should provide input to future system enhancements and change management decisions.

E3.5.3.1.1. In some cases, the CA may uncover security deficiencies, but continue to believe that the short-term system operation will present no unacceptable risks. The CA may recommend accreditation with the understanding that deficiencies will be corrected in a specified period. These deficiencies shall be reflected in the SSAA and an agreement obtained on the conditions under which the system may be operated and the date by when the deficiencies will be remedied.

E3.5.3.1.2. If the CA determines that the system does not satisfy the SSAA and that short-term risks are unacceptable, the CA shall recommend that the IT system not be accredited.

E3.5.4. DAA Accreditation Decision. The CA's recommendation, the DAA authorization to operate, supporting documentation, and the SSAA form the accreditation package. The supporting documentation may vary between system classes. That documentation, at minimum, shall include security findings and deficiencies and risks of operation. The accreditation

package must contain all information necessary to support the recommended decision. If the decision is to accredit, the decision shall include the security parameters under which the information system in its computing environment is authorized to operate. If the system does not meet the requirements stated in the SSAA, but mission criticality mandates that the system become operational, a temporary approval may be issued. Use of the temporary approval requires a return to phase 1 to negotiate accepted solutions, schedule, necessary security actions, and milestones.

E3.5.4.1. When the system accreditation has been issued, the acquisition organization normally will move the responsibility for the SSAA to the system operator or the maintenance organization for the information system. When a decision is made to accredit the system, the DITSCAP begins phase 4. If the DAA withholds accreditation, the decision shall state the specific reasons for denial and, if possible, provide suggested solutions. The DITSCAP then reverts to phase 1 to resolve the issues.

E3.5.4.2. Since it is difficult to accredit mobile systems at all possible locations, the DAA may issue a generic accreditation for a typical operating environment. The generic accreditation is the official authorization to employ identical copies of a system in a specified environment. The SSAA shall be modified to include a statement of residual risk and clearly define the intended operating environment. The SSAA shall identify specific uses of the system, operational constraints and procedures under which this system may be operated. In that case the DAA would include a statement with the accreditation, such as, “This system is supplied with a generic accreditation. With the generic accreditation, the operators assume the responsibility to monitor the environment for compliance with the environment as described in the accreditation documentation.”

E3.6. Phase 4, Post Accreditation.

E3.6.1. Phase 4 contains process activities necessary to continue to operate and manage the system so that it will maintain an acceptable level of residual risk, figure E3-12. Post-accreditation process activities shall include ongoing maintenance of the SSAA, system operations, change management, and compliance validation.

E3.6.1.1. Phase 4 begins after the system has been integrated into the operational computing environment and accredited. Phase 4 shall continue until the information system is removed from service, a major change is planned for the system, or a periodic compliance validation is required. In the first case, the DITSCAP responsibilities of the acquisition organization shift to the system manager or designated maintenance organization. In the other two cases, the DITSCAP reverts to phase 1.

Figure E3-12. DITSCAP Phase 4, Post Accreditation.

E3.6.2. Maintenance of the SSAA. As in the preceding phases, the SSAA shall be kept current. Phase 4 shall begin with a review of the SSAA to ensure that all requirements and agreements are still applicable. The user representative, the DAA, the CA, and the program manager must approve revisions to the SSAA. On approval the necessary changes to the mission, environment, and architecture are documented in the SSAA. Figure E3-13 summarizes the SSAA maintenance tasks.

Figure E3-13. SSAA Maintenance Tasks.

SSAA Maintenance Tasks

1. Review SSAA.

2. Obtain approval of changes.

3. Document changes.

E3.6.3. System Operation. The second process activity of phase 4, system operation, concerns the secure operation of the IT system and the associated computing environment, figure E3-14. System maintenance tasks ensure that the IT system continues to operate within the stated parameters of the accreditation. Secure system management depends on the organization and its procedures. Site operations staff and the ISSO are responsible for maintaining an acceptable level of residual risk. That is done by addressing security considerations when changes are made to either the information system baseline or to the baseline of the computing environment operational site. The ISSO is responsible for determining the

extent that a change affects the security posture of either the information system or the computing environment, for obtaining approval of security-relevant changes, and for documenting the implementation of that change in the SSAA and site operating procedures. Users are responsible for operating the system under the security guidelines established in the SSAA.

Figure E3-14. System Operation Tasks.

System Operation Tasks

1. System maintenance.

2. System security management.

3. Contingency planning.

E3.6.3.1. Secure system management is an ongoing process that manages risk against the IT, the computing environment, and its resources. Effective management of the risk continuously evaluates the threats that the system is exposed, evaluates the capabilities of the system and environment to minimize the risk, and balances the security measures against cost and system performance. Secure system management preserves the acceptable level of residual risk based on the relationship of mission, environment, and architecture of the information system and it's computing environment. Secure system management is a continuous review and approval process that involves the users, ISSOs, acquisition or maintenance organizations, and the DAA.

E3.6.3.2. Contingency planning is the task that develops a plan for emergency response, backup operations, and post-disaster recovery. That task shall ensure the availability of critical resources that will support the continuity of operations in an emergency situation. The operations and maintenance organizations, with the knowledge and approval of the ISSO, should develop contingency plans.

E3.6.4. Change Management. After an IT system is approved for operation in a specific computing environment, changes to the IT system and the computing environment must be controlled, figure E3-15. While changes may

adversely affect the overall security posture of the infrastructure and the IT system, change is ongoing as it responds to the needs of the user and new technology developments. As the threats become more sophisticated or focused on a particular asset, countermeasures must be strengthened or added to provide adequate protection. Therefore, change is required to maintain an acceptable level of residual risk.

Figure E3-15. Change Management Tasks.

Change Management Tasks

1. Support system configuration management.

2. Risk-based management review

E3.6.4.1. Accreditation is based on security assumptions that tie certified hardware and software of each system to the configuration of the computing environment. Changes in the information system configuration, operational mission, computing environment, or to the computing environment's configuration may invalidate the security assumptions.

E3.6.4.2. The ISSO and system users shall support the system configuration management process. They shall be involved in the change management process to ensure that changes do not have an adverse affect on the security posture of the system and it's associated IT. The strategy for managing change shall be defined in the SSAA. The ISSO shall review and approve changes relating to security and document the implementation of a change in the SSAA. Changes that significantly affect the system security posture must be forwarded to the DAA, the CA, the user representative, and the program manager (phase 1 of the DITSCAP).

E3.6.5. Compliance Validation. Periodic review of the operational system and its computing environment shall occur at the predefined intervals, defined in the SSAA. 7 The purpose of this process activity, figure E3-16, is to ensure the continued compliance with the security requirements, current threat assessment, and concept of operations as stated and agreed on in the SSAA. The compliance review should ensure that

the contents of the SSAA adequately address the functional environment into which the IT has been placed.

Figure E3-16. Compliance Validation Tasks.

Compliance Validation Tasks

1. Physical security analysis.

2. Review the SSAA.

3. Risk-based management review.

4. Procedural analysis.

5. Compliance reverification.

7 OMB, DoD, Service, and Agency directives have mandatory recertification and reaccreditation requirements. These requirements shall be included in the SSAA, governing security requisites.

E4. ENCLOSURE 4

MANAGEMENT APPROACH

E4.1. MANAGEMENT OVERVIEW

E4.1.1. The management approach for DITSCAP focuses on management at the applicable systems level to execute DITSCAP for a given system. 8 The management concept integrates existing roles in the C&A process. The concept includes system program or operations management, senior operational staff, users, and working level security managers. The DITSCAP provides visibility into the process to all mangers responsible for system development, operation, maintenance, security, and to system users.

E4.1.1.1. The key roles in the DITSCAP are the system program manager, the DAA, the CA, and the user representative. The program manager represents the interests of the system acquisition or maintenance organization with engineering, schedule, and funding responsibility; or the system operations organization with responsibility for daily operations, performance, and maintenance. The organization the program manager represents is

usually determined by the phase in the life-cycle of the system. The DAA is usually a senior operational commander with the authority and ability to evaluate the operational needs for the system in view of the security risks. The DAA must have the authority to oversee the operations and use of systems under his/her purview. The DAA represents the interests of mission need, controls the operating environment, and defines the system level security requirements. The CA provided the technical expertise to conduct the certification. The interests of the systems users are vested in the user representative. In the DITSCAP process, the user representative, at minimum, is concerned with system availability, access, integrity, functionality, and performance.

8 This description does not attempt to define the management structure within the Department of Defense, Services, or Agencies that may be necessary to oversee the C&A of DoD systems.

E4.1.1.2. These managers cooperate to provide the most capable IT system with an acceptable (tolerable) level of risk. They, and their staff, develop and approve the security requirements, manage the C&A process, and review the results. The DITSCAP allows these four managers to tailor and scope the C&A efforts to the particular mission, environment, system architecture, threats, funding, schedule, and criticality of the system. That standard approach establishes the ability to reuse both the technical and non-technical analysis, documentation, and architecture from certification or recertification efforts for similar systems.

E4.2. DITSCAP MANAGEMENT ROLES AND FUNCTIONS

E4.2.1. The organizations involved in the development, fielding, operation, and maintenance of secure IT systems include the acquisition and maintenance organizations, system operator(s), DAA(s), and the users. The key roles in these organizations involved in the C&A process, are the program manager of the organization responsible for the system i.e., the system owner, the DAA, the CA, and the user representative. The organization with engineering and funding responsibility for the system, may change, as a system progresses through the

life-cycle phases. During acquisition, this responsibility may be the acquisition organization that will be represented by the system's acquisition program manager. During the system's operations and maintenance phase that responsibility may be the system manager. In the case of a major upgrade, the system may be turned over to a maintenance organization. The upgrade program manager would then represent the maintenance organization. The DAA should be a senior member of the operational chain-of-command where the system is operating. The system users may be part of a single organization or a large diverse community. In either situation, for DITSCAP purposes, the user representative will represent the users interests.

E4.2.1.1. The key parties throughout the DITSCAP are the program manager, the DAA, the CA, and the user representative. They shall reach agreement during phase 1 "negotiation" and approve the SSAA. During phases 2, 3, and 4, if the system is changed, or any of the agreements delineated in the SSAA are modified, the four key parties return to phase 1 negotiation and subsequent revision of the SSAA.

E4.2.1.2. The CA, the ISSO, the threat developer, and the security working groups shall support the C&A process. They provide the security technical expertise to support the DAA, the program manager, and the user representative.

E4.2.1.3. The DITSCAP roles, shown in table E4-1, are described in paragraphs E4.2.2. through E4.2.4. below. The discussion describes the functional relationships and integration of these roles, but is not intended to describe organization or command functions. During the life-cycle of a system, some of these roles may be assumed by a variety of organizations. In some cases, the three roles may be performed by three separate organizations. In other cases, some roles may be combined; i.e., the user representative and the program manager roles may be performed in the same organization.

Table E4-1. Management Responsibilities by DITSCAP Phase.

Phase

Program Manager

DAA and CA

User Representative

Phase 1

Initiate security dialogue with DAA, the CA, and the user representative.

Define system schedule and budget.

Define and/or validate system performance, availability, and functionality requirements.

Support DITSCAP tailoring and level of effort determination.

Draft or support drafting of the SSAA.

Reach agreement on the SSAA.

Approve the SSAA.

Define ITSEC accreditation requirements.

Obtain threat assessment.

Begin vulnerability and risk assessments.

Assign the CA.

Support DITSCAP tailoring and determine the level of effort.

Draft or support drafting of the SSAA.

Reach agreement on the SSAA.

Approve the SSAA.

Validate and/or define system performance, availability and functionality requirements.

Support DITSCAP tailoring and level of effort determination.

Reach agreement on the SSAA.

Approve the SSAA.

Phase 2

Review the SSAA.

Develop system or system modifications.

Support certification actions.

Review certification results.

Revise system as applicable.

Review the SSAA.

Evaluate developing system.

CA performs certification actions.

CA assesses vulnerabilities.

CA reports results to the program manager, the DAA, and the user representative.

Maintain the SSAA.

Review the SSAA.

Support certification actions.

Support certification actions.

Table E4-1. Management Responsibilities by DITSCAP Phase.

Phase

Program Manager

DAA and CA

User Representative

Phase 3

Review the SSAA.

Test integrated system.

Support certification actions.

Review certification results.

Revise system as applicable.

Support SSAA revisions.

Review the SSAA.

Evaluate developing system.

CA performs certification actions.

Assess vulnerabilities and residual risk.

CA reports results to the program manager, the DAA, and the user representative.

CA develops recommendation to the DAA.

CA prepares accreditation package.

Review the SSAA.

Issue decision.

Review the SSAA.

Support certification actions.

Review certification results.

Support SSAA revisions.

Phase 4

Review SSAA periodically.

Operate system as described in the SSAA.

Maintain an acceptable level of residual risk.

Submit proposed changes to the user representative, the ISSO, the DAA, and the CA, as applicable.

Support compliance validation.

Review the SSAA.

Review proposed changes

Oversee compliance validation.

Review the SSAA.

Oversee system operation as described in the SSAA.

Maintain an acceptable level of residual risk.

Continuously review threat, system vulnerabilities and residual risk.

Review and approve proposed changes.

Submit significant changes to the DAA and the CA.

Perform compliance validation actions.

E4.2.2. Program Management Roles. The acquisition and/or maintenance organizations are responsible for IT system requirements development, architecture, design, procurement, fielding, maintenance and configuration management. The acquisition organization, figure E4-1, is the lead government organization responsible for the development and fielding of IT. After fielding, the system operator will normally designate a system manager (program manager) to oversee the operations and management of the system. If the system is formally turned over to a maintenance organization, the maintenance organization assumes the roles and functions previously assigned to the acquisition organization. The program manager is the lead for all these activities with responsibilities for cost, schedule, and performance responsibilities.
The program manager's function in the DITSCAP is to ensure security requirements are integrated into the IT architecture in a way that will result in an acceptable

level of risk to the operational infrastructure. The program manager, the DAA, and the CA shall coordinate their efforts to determine which organization will prepare the initial SSAA.

Figure E4-1. Acquisition and Maintenance Organization Program Manager Security Management Relationships.

E4.2.2.1. The PM works directly with the development integration, maintenance, configuration management, quality assurance, test independent verification and validation, and SETA organizations. The PM drafts or supports the drafting of the SSAA and coordinates security requirements with the DAA, the CA, and the user representative. The PM continuously keeps all DITSCAP participants informed of acquisition and development action, security requirements, and user needs.

E4.2.3. Security Roles and Responsibilities. Execution of the DITSCAP encompasses multiple security roles, figure E4-2, that at minimum include the DAA, the CA, and the ISSO. Additionally various security support teams may be formed to support the C&A of large systems. Together these roles establish an IT system security posture that will operate at an acceptable level of residual risk to the Department of Defense.

E4.2.3.1. The DAA is the official responsible for ensuring that IT systems provide an acceptable level of risk in the operational computing environment. In reaching that decision, the DAA is supported by the CA, threat developer, ISSO, and security teams. Those roles shall evaluate the technical and non-technical aspects of the design, installation, and operation of the IT system. They also shall support the evaluation of the impact of the operation of the system on the security posture of the DII. From the perspective of a single system, all security related organizations support the DAA.

Figure E4-2. Security Management Relationships.

E4.2.3.2. The DAA shall coordinate the development of the initial SSAA with the program manager. The initial SSAA may be prepared by either organization. In phase 2 and 3 the responsibility for the SSAA updates, maintenance and addition of the certification results

shall become the responsibility of the CA. Where the IT system may involve multiple DAAs, agreements shall be established between the cognizant DAAs. Those agreements form an integral portion of the SSAA. In most cases, it will be advantageous to designate a lead DAA to represent the DAAs in developing and maintaining the IT system.

E4.2.3.3. The CA shall support the DAA for the comprehensive evaluation of the technical and non-technical security features of the IT system. When tasked by the DAA, the CA is responsible for preparation of the SSAA, and the software, hardware, TEMPEST, COMSEC, physical, and procedural evaluations. The CA shall be independent from the organization responsible for the system. Organizational independence of the CA eases the potential of conflicts of interest and permits an impartial evaluation.

E4.2.3.4. The CA shall have staff who are technically knowledgeable in IT system design, security design, and the security policies and procedures that satisfy the ITSEC requirements. Although all the technical capabilities may not be available in the CA's organization, the CA is responsible for obtaining the necessary support and providing the necessary oversight of the certification effort. Security teams may be formed to support the C&A or any portion of the process; e.g., security testing. The composition, roles, responsibilities, schedule, and funding of those teams should be defined in the SSAA.

E4.2.3.5. The ISSO is responsible for the secure operation of the system. The ISSO responsibilities will be discussed in the next section.

E4.2.4. User Roles and Responsibilities. The IT system user resides in a computing environment with either direct or indirect accesses to the information and IT system resources that comprise the computing environment's infrastructure. Users are at all levels and echelons within DoD. The users are responsible for the identification of the operational requirements and the secure operation of certified and accredited IT systems, in accordance with the SSAA.

Figure E4-3. User Community Management Relationships.

E4.2.4.1. The user representative is the liaison for the user or the user community, particularly during the initial development of a system. The user representative, figure E4-3, is the individual or organization that represents the user community in the specification, acquisition and maintenance of IT system. The user representative defines the system mission and functionality and is responsible for ensuring that the user's interests are maintained throughout system development, modification, integration, acquisition, and deployment.

E4.2.4.2. The security focal point in the user community is usually the ISSO who is responsible for the secure operation of the IT system within the environment agreed on in the SSAA. The ISSO ensures the IT system is employed and operated according to the SSAA through integration of all the security disciplines (COMPUSEC, COMSEC, EMSEC, personnel, physical, and administrative procedures) to maintain an acceptable level of residual risk.

E4.2.4.3. Since the operational scenarios in the DoD Components may vary to a wide degree, the exact location and number of ISSO(s) in a single command or Agency may vary. ITSEC management may require a single ISSO to coordinate the actions of IT systems at multiple sites or environments, or may require the appointment of an ISSO for each site or environment. User organizations shall assign the ISSO(s) to an organizational position where the ISSO has direct access to applicable decision makers. The ISSO shall not be directly assigned to the organization responsible for the daily IT system operations. The ISSO should be separate from the system administration organization but at an equal level within the information resource management unit.

E5. ENCLOSURE 5

ACRONYMS AND ABBREVIATIONS

E5.1. Acronyms and abbreviations

The acronyms and abbreviations in this enclosure are used throughout this instruction.

E5.1.1.

ASAP

As soon as possible

E5.1.2.

CA

Certification Authority

E5.1.3.

C&A

Certification and Accreditation

E5.1.4.

CINC

Commander-in-Chief

E5.1.5.

COMPUSEC

Computer Security

E5.1.6.

COMSEC

Communications Security

E5.1.7.

CONOPS

Concept of Operations

E5.1.8.

COTS

Commercial Off-The-Shelf

E5.1.9.

CRLCMP

Computer Resources Life-Cycle Management Plan

E5.1.10.

CRMP

Computer Resource Management Plan

E5.1.11.

CRR

Certification Requirements Review

E5.1.12.

DAA

Designated Approving Authority

E5.1.13.

DCID

Director of Central Intelligence Directive

E5.1.14.

DGSA

DoD Goal Security Architecture

E5.1.15.

DII

Defense Information Infrastructure

E5.1.16.

DITSCAP

DoD Information Technology Security Certification and Accreditation Process

E5.1.17.

EMSEC

Emissions Security

E5.1.18.

GOTS

Government Off-The-Shelf

E5.1.19.

IASE

Information Assurance Support Environment

E5.1.20.

INFOSEC

Information System Security

E5.1.21.

ISSO

Information Systems Security Officer

E5.1.22.

IT

Information Technology

E5.1.23.

ITSEC

Information Technology Security

E5.1.24.

NDI

Non-Developmental Item

E5.1.25.

NSTISSI 4009

National Telecommunications and Information Systems Security (INFOSEC) Glossary

E5.1.26.

OMB

Office of Management and Budget

E5.1.27.

OSD

Office of the Secretary of Defense

E5.1.28.

SCI

Sensitive Compartmented Information

E5.1.29.

SETA

Systems Engineering, Testing, and Analysis

E5.1.30.

SSAA

System Security Authorization Agreement

E5.1.31.

ST&E

Security Test and Evaluation

E5.1.32.

TAFIM

Technical Architecture Framework for Information Management

E6. ENCLOSURE 6

SSAA OUTLINE

E6.1. SSA outline

The SSAA is a living document that represents the formal agreement among the DAA, the CA, the user representative, and the program manager. The SSAA is developed in phase 1 and updated in each phase as the system development progresses and new information becomes available. At minimum, the SSAA should contain the information in the following sample format:

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1. System name and identification.

1.2. System description.

1.3. Functional description.

1.3.1. System capabilities.

1.3.2. System criticality.

1.3.3. Classification and sensitivity of data processed.

1.3.4. System user description and clearance levels.

1.3.5. Life-cycle of the system.

1.4. System CONOPS summary.

2. ENVIRONMENT DESCRIPTION

2.1. Operating environment.

2.2. Software development and maintenance environment.

2.3. Threat description.

3. SYSTEM ARCHITECTURAL DESCRIPTION

3.1. Hardware.

3.2. Software .

3.3. Firmware .

3.4. System interfaces and external connections.

3.5. Data flow (including data flow diagrams).

3.6. TAFIM DGSA, (reference (m)), security view.

3.7. Accreditation boundary.

4. ITSEC SYSTEM CLASS

4.1. Interfacing mode.

4.2. Processing mode.

4.3. Attribution mode.

4.4. Mission-reliance factor.

4.5. Accessibility factor.

4.6. Accuracy factor.

4.7. Information categories.

4.8. System class level.

4.9. Certification analysis level.

5. SYSTEM SECURITY REQUIREMENTS

5.1. National and DoD security requirements.

5.2. Governing security requisites.

5.3. Data security requirements.

5.4. Security CONOPS.

5.5. Network connection rules.

5.5.1. To connect to this system.

5.5.2. To connect to the other systems defined in the CONOPS.

5.6. Configuration and change management requirements.

5.7. Reaccreditation requirements.

6. ORGANIZATIONS AND RESOURCES

6.1. Identification of organizations.

6.1.1. DAA.

6.1.2. CA.

6.1.3. Identification of the user representative.

6.1.4. Identification of the organization responsible for the system.

6.1.5. Identification of the program manager or system manager.

6.2. Resources.

6.2.1. Staffing requirements.

6.2.2. Funding requirements.

6.3. Training for certification team.

6.4. Roles and responsibilities.

6.5. Other supporting organizations or working groups.

7. DITSCAP PLAN

7.1. Tailoring factors.

7.1.1. Programmatic considerations.

7.1.2. Security environment.

7.1.3. IT system characteristics.

7.1.4. Reuse of previously approved solutions.

7.1.5. Tailoring summary.

7.2. Tasks and milestones.

7.3. Schedule summary.

7.4. Level of effort.

7.5. Roles and responsibilities.

Appendices shall be added to include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation that will be relevant to the systems' C&A.

APPENDIX A. Acronym list

APPENDIX B. Definitions

APPENDIX C. References

APPENDIX D. Security requirements and/or requirements traceability matrix

APPENDIX E. Security test and evaluation plan and procedures

APPENDIX F. Certification results

APPENDIX G. Risk assessment results

APPENDIX H. CA’s recommendation

APPENDIX I. System rules of behavior

APPENDIX J. Contingency plan(s)

APPENDIX K. Security awareness and training plan

APPENDIX L. Personnel controls and technical security controls

APPENDIX M. Incident response plan

APPENDIX N. Memorandums of agreement - system interconnect agreements

APPENDIX O. Applicable system development artifacts or system documentation

APPENDIX P. Accreditation documentation and accreditation statement

E7. ENCLOSURE 7

ITSEC SYSTEM CLASS DESCRIPTION

E7.1. INTRODUCTION

E7.1.1. Within the Department of Defense, IT systems perform a wide variety of functions to ensure a mission is accomplished and harm is prevented. The information and processes used to perform those functions, regardless of their classification, helps the Department of Defense to operate more efficiently and accomplish its missions. The information and processes shall be afforded an applicable level of protection for confidentiality, integrity, availability, and accountability. Determination of the proper level of protection shall be based on the perceived value of the information and processes. That value is related to the adverse impact, either fiscal, or operational, or both that the loss, alteration, denial of access, or unauthorized access have on DoD missions.

E7.1.2. Security requirements have been established to ensure that information systems provide the required degree of protection. The security requirements are primarily a function of the system mission (operational

functions and data processed; etc.), environment (operating and maintenance environment; i.e., the physical and procedural controls for using the system), and architectural concept (stand-alone system, networked and distributed processing; etc.). The degree that systems comply with security requirements produces a level of assurance that the specific information will be protected commensurate with its value to the Department of Defense. The evaluation of information systems to determine the level of assurance requires knowing the ITSEC policy, the way systems permit access to information, and the operational environment for the systems.

E7.1.3. Even though specifics for any given system may, or will differ, these groupings allow one to consider and reuse issues, risks, requirements, solutions, implementations, and analyses from other systems within its class or in related tasks. They provide the ability to compare and contrast systems both within a class or in related tasks. That class structure bounds the security problem and permits security requirements to be grouped to satisfy individual class conditions.

E7.1.4. Technology now provides the Department of Defense with the ability to distribute IT processing locations and access the information processing points from anywhere in the world. It is now possible for one information system to affect other widely distributed systems and the security qualities of confidentiality, integrity, availability, and accountability anywhere in the world. Connection to the communications infrastructure is a prime consideration in evaluating risk. The ITSEC class structure considers a systems security posture as both a single entity and in relationship to other systems.

E7.2. ITSEC CLASSES

E7.2.1. An ITSEC system class is a profile of system characteristics derived from considering how the same characteristics applied to the system's operation data affects community mission outcome. System classes group information systems with others of similar missions, operating environments, architectures, and data. Systems are grouped by their interaction with other systems, the way that users and processes must access different

types of data, and the security policies that control access of specific information categories. The intent is to group systems by the amount of risk exposure within the system; i.e., capability to contain risk. Members of a class may share common security policies, requirements, and levels of assurance.

E7.2.1.1. Grouping systems into classes provides many benefits over examining each system on its own merits and determining the individual security requirements to satisfy the specific problem. Examining each system as a single entity is time consuming and resource intensive. Experience has shown that similar systems, information processed, and environment, exhibit similar security requirements to provide an acceptable level of residual risk. Establishing a common set of criteria permits a class repository to be established so that new developments may draw from applicable past experience. That will allow security policy to be determined rapidly and security requirements to be assigned quickly, based on the group or class into which the system falls. This more economical approach supports standardization by grouping systems into categories of similar risk. It also promotes the development of common or reusable security solutions because all systems of a class will share common mission, policy, data, and security requirements. When a new system development begins, or an existing system is to be revised, the class repository may be accessed to obtain the policy and security requirements. This should eliminate the need for lengthy meetings to define the security policy and requirements. The class repository also may provide lessons learned relative to successful security architectures, certification approaches, and tools used. However, it will not delete any of the activities required to determine if the system may be certified. Nor shall system class membership eliminate the system engineering tradeoff decisions between implementation of physical controls and technical countermeasures.

E7.2.1.2. The ITSEC class decision process shall begin by considering the impact of the IT system on other systems. It shall then consider system user interaction, mission, and data types. To consider the impact on other systems, the risk of the specific system to other systems must be accessed. That approach to ITSEC evaluation and C&A focused on infrastructure, shall determine the

universal risk to other systems, not just the specific system under consideration.

E7.2.1.3. Table E7-1 provides a form for determining the ITSEC class for a system. It resolves several security discriminating characteristics for a system by first considering the same characteristics for the operation and data associated with the system. This shall be done with direct consideration of the infrastructure where the system is connected. The characteristics for the system shall be chosen to be adequate to accommodate the operation, the data, and associated infrastructure considerations. The characteristics include; interfacing mode, processing mode, attribution mode, accessibility factor, accuracy factor, and information categories. Specific alternatives are selectable for each characteristic shown in table E7-1.

Table E7-1. ITSEC Class Characteristics.

Characteristic

Operation

Data

Infra-

structure

System

Alternatives

Interfacing Mode

Benign, Passive, or Active

Processing Mode

Dedicated Level, Compartmented Level, System High, or Multi-level

Attribution Mode

None, Rudimentary, Basic, or Comprehensive

Mission-Reliance Factor

None, Cursory, Partial, or Total

Accessibility Factor

Reasonable, Soon, ASAP, or Immediate

Accuracy Factor

Not-applicable, Approximate, or Exact

Information Categories

Unclassified, Sensitive (Privacy Act, Financially Sensitive, Administrative, Proprietary, or Other), Collateral Classified, or Compartmented/Special Access Classified

E7.2.1.4. The selections for each characteristic will associate systems with similar security requirements for C&A. The concept of class implies that systems and associated C&A activities may be grouped. Classes permit the comparison of systems and use of previous experience from systems in the same or similar classes.

E7.2.2. Interfacing Mode. The interfacing mode categorizes interaction. The question concerns containment of risk; e.g., if a problem were to occur with the operation, data, or system, what would be the risk to other operations, data, or systems with that it interacts, respectively. The interactions of systems may be through either physical or logical relationships. Those relationships are referred to as benign, passive, or active.

E7.2.2.1. Benign. Connotes free of interaction; i.e., no physical or logical relationships. All relationships are restricted to a closed community.

E7.2.2.2. Passive. Connotes limited to indirect interaction, and may or may not have physical relationships, but with tightly controlled logical relationships. An example is a terminal with receive only sessions. (The passive case permits lower-level protocols to support passive interactions.)

E7.2.2.3. Active. Connotes direct interaction, with both physical and logical relationships. The active case may allow multiple interactive sessions with multiple operations, systems, infrastructures, or data.

E7.2.3. Processing Mode. The processing mode distinguishes the way processing, transmission, storage, or data is handled. It reflects the use of the system by one or more different sets of users or processes. The alternatives are: dedicated level, compartmented level, system high level, and multi-level. Each of the modes exhibit unique security qualities.

E7.2.3.1. Dedicated Level. Connotes processing, transmission, or storage is within a single information category. (All users and processes have a valid security clearance for all processes and data, and all users or processes have the same need to know. Access controls are equal for all users and processes.)

E7.2.3.2. Compartmented Level. Connotes that processing, transmission, storage, or data is handled across different information categories with single-level access by individual users or processes at any "given time." (All users and processes have a valid clearance for the most restricted information processed in the system, and a valid need-to-know for the information that the user or process will have access. Access controls are different for each user and process.)

E7.2.3.3. System High. Connotes that processing, transmission, storage, or data while actually across different information categories, is handled as if it were in a single information category or processing domain. (All users and processes have valid security clearance to all processes and data. All users and processes may not have the same need to know. Access controls are equal for all users and processes.)

E7.2.3.4. Multilevel. Connotes that processing, transmission, storage, or data is handled across different information categories with "simultaneous" access by individual users or processes. (All users and processes may not have the same clearances or need to know. Access controls are different for each user and process.)

E7.2.4. Attribution Mode. The attribution mode distinguishes the degree or complexity of accountability required to establish authenticity and nonrepudiation. Four alternatives are: rudimentary, selected, and comprehensive.

E7.2.4.1. None. Means no processing, transmission, storage, or data carries the ability to attribute them to users or processes.

E7.2.4.2. Rudimentary. Means the most basic processing, transmission, storage, or data carries the ability to attribute them to users or processes.

E7.2.4.3. Selected. Means some processing, transmission, storage, or data carries the ability to attribute them to users or processes.

E7.2.4.4. Comprehensive. Means all or almost all processing, transmission, storage, or data carries the ability to attribute them to users or processes.

E7.2.5. Mission-Reliance Factor. The mission-reliance factor relates the degree that the success of the mission relies on the operation, data, infrastructure, or system. The criticality of the mission in a broader context is independent of that factor and is used separately. Four alternatives selectable are: none, cursory, partial, or total.

E7.2.5.1. None. Means that the mission is not dependent on the specific aspect; i.e., the operation, data, infrastructure, or system.

E7.2.5.2. Cursory. Means that the mission is dependent on the specific aspect; i.e., the operation, data, infrastructure, or system, is cursory.

E7.2.5.3. Partial. Means that the mission is partially dependent on the specific aspect; i.e., the operation, data, infrastructure, or system.

E7.2.5.4. Total. Means that the mission is totally dependent on the specific aspect; i.e., the operation, data, infrastructure, or system.

E7.2.6. Accessibility Factor. The accessibility

factor relates the degree that the operation, data, infrastructure, or system needs to be available from a security perspective. Here, availability concerns are those that relate to security risks; i.e., non-tolerable operational impacts, and does not include those that are only performance concerns. Four alternatives are selectable: reasonable, soon, ASAP, or immediate.

E7.2.6.1. Reasonable. Means that the specific aspect; i.e., the operation, data, infrastructure, or system, must be available in reasonable time to avoid operational impacts.

E7.2.6.2. Soon. Means that the specific aspect; i.e., the operation, data, infrastructure, or system, must be available soon (timely response) to avoid operational impacts.

E7.2.6.3. ASAP. Means that the specific aspect; i.e., the operation, data, infrastructure, or system, must be available as soon as possible (quick response) to avoid operational impacts.

E7.2.6.4. Immediate. Means that the specific aspect; i.e., the operation, data, infrastructure, or system, must be available immediately (on demand) to avoid operational impacts.

E7.2.7. Accuracy Factor. The accuracy factor relates the degree that the integrity of operation, data, infrastructure, or system is needed from a security perspective. Here, integrity concerns are those that relate to security risks; i.e., non-tolerable operational impacts, and does not include those that are only performance concerns. Three alternatives are selectable: not-applicable, approximate, or exact.

E7.2.7.1. Not-Applicable. Means that the degree of integrity for a specific aspect; i.e., the operation, data, infrastructure, or system, is irrelevant as to operational impacts.

E7.2.7.2. Approximate. Means that the degree of integrity for a specific aspect; i.e., the operation, data, infrastructure, or system, must be approximate in order to avoid operational impacts.

E7.2.7.3. Exact. Means that the degree of integrity for a specific aspect; i.e., the operation, data, infrastructure, or system, must be exact in order to avoid operational impacts.

E7.2.8. Information Category. The mission of each system will determine the information that is processed. The mission and information will influence the environment and security requirements applicable to each information category. Information categories are defined by their relationships with common management principles and security requirements promulgated by the security policy for each information category. Processing, transmission, storage, and data of more than one category of information shall not create a new category but shall instead inherit and shall satisfy all the security requirements of the assigned categories. Each of the identified categories may carry additional restrictions or special handling conditions; e.g., NATO-releasable or NOFORN. The information categories are defined as follows:

E7.2.8.1. Unclassified. This category of information includes all information that is not classified and is not sensitive as defined in paragraph E7.2.8.2. below.

E7.2.8.2. Sensitive Information. This category includes information, the loss misuse, or unauthorized access to or modification that could adversely affect the national interests or the conduct of federal programs, or the privacy that individuals are entitled under 5 U.S.C. 552a (reference(l)), but that has not been specifically authorized under criteria established by an E. O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the Pub. L. 100-235 (reference(b)).
In many cases, it may be useful to further characterize the sensitive information by determining the subcategory. This may indicate additional national, DoD, Service, or Agency requirements that are imposed by processing that type of information. The subcategories are:

E7.2.8.2.1. Privacy Act. This category includes all information covered by reference (l) and also includes

medical, pay, personnel information, etc. Information may be either classified or unclassified. Privacy Act information requires handling according to a common sensitivity. Privacy Act information usually requires system and information access control.

E7.2.8.2.2. Financially Sensitive. This category includes financially and contractually sensitive information. Information may be either classified or unclassified. Financially sensitive category information requires handling according to a common sensitivity, and may require special assurance mechanisms such as two-person verification of transactions. Financially sensitive category information requires system and information access control.

E7.2.8.2.3. Proprietary. This category includes information provided by a source or sources under the condition that it not be released to other sources. This information may require system or information access control.

E7.2.8.2.4. Administrative and/or Other. This category includes DoD information associated with housekeeping activities, information marked For Official Use Only, and unclassified information that does not fall into any of the other information categories.

E7.2.8.3. Collateral Classified. This category includes all classified information not included in the Compartmented and/or Special Access Category.

E7.2.8.4. Compartmented and/or Special Access Classified. This category includes all information that requires special access and a security clearance. Examples include sensitive compartmented information, Single Integrated Operations Plan-Extremely Sensitive Information, and special access programs.

E7.2.9. Each of the identified categories may carry additional restrictions or special handling conditions; e.g., NATO-releasable or NOFORN.

E7.3. SECURITY REQUIREMENTS

E7.3.1. Successful implementation of secure systems

depends on defining security requirements early. All ITSEC disciplines (COMPUSEC, COMSEC, EMSEC, physical, and personnel) must be considered in the requirements definition process to arrive at a complete set of requirements. This permits the program manager, the user representative, and the DAA to evaluate cost versus risk tradeoffs successfully and assign security requirement implementation to hardware or software components, or procedures.

E7.3.2. While all systems share a common set of minimum security requirements, some systems will inherit additional requirements based on their mission and function. Additionally, some systems, based on mission and function, may need a higher level of assurance that security requirements have been implemented successfully. That is a basic distinction among the classes.

E7.3.3. When a system is identified with a class of similar systems, the class repository may be accessed for a common set of ITSEC requirements. This eliminates the need for the program manager of each system to develop the security requirements independently from myriad security instructions and directives and forward them to the DAA for approval. The question then remains, how will these requirement sets be developed?

E7.3.4. The approach is twofold.

E7.3.4.1. Existing systems will be analyzed to determine their classes. Those systems that have been accredited may be used as "models" for others of the class. Their ITSEC requirements, high-level architectures and approved solutions may be documented in a common repository. When a new system is required in that class, or a legacy system needs to be upgraded, the class repository will provide valuable support.

E7.3.4.2. An independent requirements definition process needs to collect all ITSEC requirements into a common database. Then the requirements need to be reviewed to remove conflicts and duplications to produce a clean, and complete set of requirements. Those requirements may be allocated to each security class. The result will be an agreed on consistent set of security requirements for each class. Again, users of that class will have the economy of a readily obtainable requirements set.

E7.4. DETERMINATION OF SYSTEM CLASS

E7.4.1. A key step in the use of system classes is first to prepare an accurate description of the system being considered. While the details of the system may not be clear at the outset of development, its outlines and boundaries should be understood. It is important to know what is not part of the system as well as what is part of the system. The system description shall include those items in figure E7-1.

Figure E7-1. System Description Elements.

1. Mission of the system.

2. Functions this system will perform.

3. Interfaces with other systems.

4. Interactions across system interfaces.

5. Expected users of this system.

6. Information categories to be processed.

7. Time frame for developing and implementing the system.

8. Components of the system that will be automated versus manual.

9. Budget limitations that may affect the system.

10. Other system constraints or assumptions that will impact the system.

E7.4.2. These questions define the boundaries of the system compared to those that this system may interact. That description shall be sufficiently clear and comprehensive to provide an unambiguous definition of when the system may be certified and accredited. If information or understanding about the system is insufficient for that system description to be written, the DITSCAP is not ready to begin.

E7.4.3. Determining the applicable system class is essential to development of the minimal security requirements necessary for the certification and eventual accreditation of the system. By determining the applicable class, the security engineer automatically develops the minimum set of security requirements for the system being analyzed. The various system classes also are associated with specific DITSCAP activities that must be performed. As a result, early in system development the minimum set of security requirements as well as the DITSCAP activities are known to the program manager, the DAA, the user representative, and the CA.

E7.4.4. A system class is determined by first selecting the applicable entries for the first three columns of table E7-1. Next the first three entries are resolved to reflect the most applicable value for the fourth column so that the system will adequately support the needs defined in the first three columns. That will result in a system with the minimum security requirements required in the context of its associated operation, data, and infrastructure. Future DITSCAP application guidance will give further instruction with specific examples and rules in selecting the applicable alternatives for each characteristic as it applies to each system aspect. For example, a completed system class chart could look like the following.

Table E7-2. ITSEC Class Characteristics.

Characteristic

System

Alternatives

Interfacing Mode

Active

Benign, Passive, or Active

Processing Mode

System High

Dedicated, Compartmented, System High, or Multi-level

Attribution Mode

Basic

None, Rudimentary, Selected, Basic, or Comprehensive

Mission-Reliance Factor

Partial

None, Cursory, Partial, or Total

Accessibility Factor

ASAP

Reasonable, Soon, ASAP, or Immediate

Accuracy Factor

Approximate

Not-applicable, Approximate, or Exact

Information Categories

Sensitive

Sensitive (U.S.C. Code 552 (reference(l)), Financially Sensitive, Administrative, Proprietary, or Other), Collateral Classified, or Compartmented and/or Special Access Classified

E8. ENCLOSURE 8

DITSCAP COMPONENTS OVERVIEW

E8.1. DITSCAP Components

The DITSCAP components are composed of phases, activities, tasks, and steps. There are four phases: Definition, Verification, Validation, and Post Accreditation. Each phase is composed of activities that are in turn composed of tasks. Each certification analysis task is composed of one or more steps as determined by the

level of certification analysis required.

E8.2. Table 8-1

Table 8-1 shows the relationship of the phases, activities and tasks.

Table 8-1. Relationship of Phases, Activities, and Tasks.

Phase

Associated Activities

Associated Task

Phase 1, Definition.

Document mission need.

Determine and document mission functions.

Conduct registration.

Register the system - inform the DAA and the user representative that a system will require C&A support.

Prepare mission description and system identification.

Prepare environment and threat description.

Prepare system architecture description.

Determine the ITSEC class.

Determine the system security requirements.

Identify organizations that will support the C&A.

Tailor the DITSCAP tasks, determine the C&A scope, level-of-effort, and prepare the DITSCAP plan.

Develop the draft SSAA.

Perform negotiation.

Review the draft SSAA.

Conduct the CRR.

Approve the SSAA.

Prepare the SSAA.

Table 8-1. Relationship of Phases, Activities, and Tasks.

Phase

Associated Activities

Associated Task

Phase 2, Verification.

Refine the SSAA.

Support system development activities.

Perform certification analysis.

System architecture analysis.

Software design analysis.

Network connection rule compliance analysis.

Integrity of integrated products analysis.

Life-cycle management analysis.

Vulnerability assessment analysis.

Assess analysis results against SSAA requirements.

Phase 3, Validation.

Refine the SSAA.

Certification evaluation of the integrated system.

ST&E.

Penetration testing.

TEMPEST and red-black verification.

Validation of COMSEC compliance.

System management analysis.

Contingency plan evaluation.

Risk-based management review.

Develop recommendation to the DAA.

CA’s recommendation.

DAA accreditation.

Phase 4, Post Accreditation.

Maintenance of the SSAA.

Review the SSAA.

Obtain approval of changes.

Document changes.

System operation.

System maintenance.

System security management.

Contingency planning.

Change management.

Support system configuration management.

Risk-based management review.

Compliance validation.

Review the SSAA.

Physical security analysis.

Procedural analysis.

Risk-based management review.